UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Black Apple iPhone, assigned telephone number ending in 0220, located in the Eastern District of Pennsylvania	)	Case No. 24-mj-1281

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1513(e)	witness retaliation
18 U.S.C. § 1512(b)(1)	witness intimidation
18 U.S.C. § 2	aiding and abetting

The application is based on these facts:
See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Lorelei Schreier
Applicant's signature

Special Agent Lorelei Schreier, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: Carol Sandra Moore Wells Date: 2024.08.07 13:55:50 -04'00'

Judge's signature

City and state: Philadelphia, Pennsylvania

Honorable Carol S. Wells, USMJ
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Black Apple iPhone, assigned telephone number ending in 0220, located in the Eastern District of Pennsylvania	)	Case No. 24-mj-1281

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before August 21, 2024 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate judge.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Carol Sandra Moore Wells Date: 2024.08.07 13:56:35 -04'00'

Judge's signature

City and state: Philadelphia, Pennsylvania Honorable Carol S. Wells, USMJ

Printed name and title

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH WARRANT

I, Lorelei Schreier, being duly sworn, do hereby depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to the Philadelphia, Pennsylvania, office. As such, I am a "federal law enforcement officer" within the meaning of the Federal Rules of Criminal Procedure 41(a)(2)(C), that is a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. As a Special Agent, I have investigated, among other things, cases involving the use of computers, cellular telephones, and the internet to commit violations of federal law involving securities fraud, wire fraud, and other financial crimes. I have also participated in the execution of warrants under the authority of the United States. I have previously obtained and executed several search warrants in furtherance of one or more investigations.

2. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records.

3. This affidavit is submitted in support of a search warrant authorizing the review and forensic examination of property—a cellular telephone—which is currently in law enforcement possession, and the extraction from that phone of the electronically stored information described in Attachment B.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the

investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to search the Subject Locations.

5. The cellular telephone that is the subject of this application is a black Apple iPhone, assigned telephone number ending in 0220, and is further described in Attachment A (the "Verne iPhone"). The Verne iPhone was obtained at the time of the August 2, 2024, arrest of Josh S. Verne in Fort Lauderdale, Florida. That arrest was pursuant to a warrant issued by the Court, in docket number 24-cr-270, upon the return of an indictment charging Verne with: (i) three counts of securities fraud; (ii) 22 counts of wire fraud; (iii) one count of aggravated identity theft; (iv) one count of witness retaliation; and (v) one count of witness intimidation.

6. The Verne iPhone is now in the Eastern District of Pennsylvania, within the jurisdiction of this Court, in a secure storage space at the Federal Bureau of Investigation, 600 Arch Street, Philadelphia, Pennsylvania. In my training and experience, I know that iPhone has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the iPhone first came into the possession of law enforcement.

7. As set forth in the indictment in docket number 24-cr-270, the witness retaliation and witness intimidation charges arise out of a "reverse proffer" meeting that I attended in person on or about September 12, 2022, along with Josh S. Verne's then-current criminal defense counsel. Verne attended that meeting by telephone by way of a speakerphone in the conference room where the meeting was being held.

8. During the course of that meeting I, along with some assistance from other government personnel, described and discussed with Verne's counsel, in Verne's presence by telephone, some of the evidence that the United States had collected in its federal criminal investigation against Verne and the implications of that evidence for our contemplated charges against Verne.

9. Among the events discussed at the reverse proffer meeting was the unauthorized sale by Verne of stock belonging to an individual, known to me but who is identified in the indictment as Employee 1. Employee 1 was a lifelong friend of Verne, whom Verne had hired as a management officer of one of his companies. As part of his compensation for his position and employment for Verne's company, Employee 1 acquired units (*i.e.* shares) in that company (the "Employee 1 Units").

10. Employee 1 resigned from Verne's company in or about February 2020. However, Employee 1 retained ownership of his shares in Verne's company after his termination of his employment with the company.

11. On or about March 9, 2020, Verne entered into an agreement to sell the Employee 1 Units to another individual. Employee 1 advised agents that this agreement was made without the knowledge or approval of Employee 1.

12. In order to consummate this unauthorized sale, a forgery of Employee 1's signature was added to the sales agreement for the Employee 1 Units, without the knowledge, permission, or approval of Employee 1. According to Employee 1, Employee 1 never agreed to this sale, Verne never discussed this sale with him, and the signature on the sales agreement was not Employee 1's signature. According to information provided

by the purchaser and a review of bank records, on or about March 9, 2020, the purchaser paid Verne approximately $150,000 for the Employee 1 Units without knowledge of the fact that Employee 1's signature had been forged on the sales agreement and that Verne did not have legal authority to transfer ownership of those units.

13. Further, according to Employee 1 and bank records, Verne never turned over to Employee 1 the approximately $150,000 that he had obtained from the sale of the Employee 1 Units. Instead, Verne misapplied those funds. According to financial documents obtained by the FBI, Verne used those funds to make a payment to (1) an earlier investor in the company from which Employee 1 had formerly worked and (2) his own bank account.

14. During the reverse proffer, I explained to the group, including Verne, that I had learned this information about Verne's unauthorized sale of the Employee 1 Units through witness interviews and that a witness had confirmed that Employee 1's signature on the sales agreement had been forged. We also discussed the fact that this evidence would establish the federal crime of Aggravated Identity Theft and that this offense carried a mandatory minimum sentence of two years imprisonment.

15. I later learned from speaking to Employee 1 that, within minutes after the conclusion of the reverse proffer meeting, Verne's cell phone number contacted Employee 1 by text message. I have seen copies of the text message. It says that its author had just gotten off the phone with the "appropriate people" to whom Employee 1 had spoken. Employee 1 did not respond to this text message.

16. According to Employee 1 and a review of Employee 1's text messages, less than two hours later, Verne's cell phone number sent Employee 1 another text message which threatened to divulge embarrassing information, about events that Employee 1 says in fact never actually happened, "[i]f this goes forward."

17. According to Employee 1's wife and a review of her text messages, later that night, Verne's cell phone number sent a text message to Employee 1's wife which said that, because Employee 1 had spoken to the "authorities" about him (allegedly supplying misinformation), Employee 1's spouse would "be brought into the conversation."

18. There is probable cause to attribute all three text messages to Verne, and that Verne used the Verne iPhone to send the messages. First, from the text message display, Employee 1's cell phone identified the incoming number as belonging to Verne and that number ending in 0220 is the number assigned to the Verne iPhone. Employee 1 told me that he was a long-time friend of Verne's and that this was the number that Verne had used to communicate with him for some time. Likewise, Employee 1's wife told me that her phone recognized the number as belonging to Verne.

19. Second, the content of the messages confirms Verne's participation. The first message, received within minutes of the end of the proffer meeting which Verne attended by phone, is written in the first person, and begins with, "Just got off the phone with the appropriate people who spoke to u." From context, I understand the "appropriate people" to mean the government in general and me in particular. This conclusion is

confirmed by the later text to Employee 1's wife, which says that her husband talked to the "authorities" about the author of the text.

20. I know from Verizon records that Verne has the same cellular telephone number and cellular phone carrier as of April 7, 2023, that he did on September 12, 2020, the date of the reverse proffer meeting.

21. I was present for Verne's arrest on August 2, 2024. When he was arrested, Verne had his cellular phone, the Verne iPhone, in his possession and used it to call his attorney. That phone is an Apple iPhone, which is a smart phone. There is probable cause to believe based on my investigation that Verne also had an iPhone in September 2020, because several people whom I interviewed received iMessages from Verne in the time period, and I know that iMessage functions exclusively on Apple platforms, including messages sent from an iPhone to an iPhone.

22. While I do not know whether the iPhone seized from Verne at the time of his arrest is the same physical phone as he had in September 2020, there is probable cause to believe that evidence relevant to the investigation will be found on Verne's phone. I know from my experience and training that smart phones (of which an iPhone is one) are designed so that data from an old phone can be quickly and easily transferred from an old phone to a new phone upon purchase. Indeed, this is an important selling point inasmuch as a laborious process of transferring data would make people reluctant to replace their old phone with newer models. In particular, in the case of iPhones, the data transfer process can be easily conducted by a consumer wirelessly by placing the new and old iPhones next to one another.

23. I also know that smart cellular telephones have very large data storage capacities. While it is possible to delete evidence of particular text messages and calls, from my experience and training I know that most people allow their phones to accumulate data unless there is a specific reason to delete it. Moreover, I also know from my experience and training that data deleted on a cellular phone can often be recovered in a forensic examination. Typically, deleted data is not wiped off of the device, but remains available for recovery by a properly trained person with the appropriate tools.

24. Given that the cellular phone that law enforcement seized from Verne at the time of his arrest is an iPhone, and given that the phone that Verne was using at the time that the reverse proffer meeting occurred and the subsequent text messages were sent was also an iPhone, there is probable cause to believe that evidence of those text messages will be on his current phone. Likewise, there is probable cause to believe that evidence of his attendance at the reverse proffer meeting may also be on that phone. Therefore there is probable cause to search for and seize: (1) evidence of phone numbers dialed and numbers that called in to Verne's cell phone number on September 12, 2020, the date of the reverse proffer meeting; and (2) text messages sent or received by Verne's cell phone number on September 12, 2020, the date of the reverse proffer meeting.

25. There is also probable cause to search for and seize evidence of user attribution showing who used or owned the Verne iPhone on September 12, 2020. If only Verne used it on that day, then it is far more likely that he was the author of the texts to Employee 1 and Employee 1's wife. For the same reasons, I seek permission to search for and seize user attribution data for three weeks before and three weeks after September 12,

2020. If Verne was the only person using his phone throughout this period, or if there is some pattern to the use by different persons, it will help to establish – or dis-establish – Verne as the author of the texts. This would allow a review, for that time period only, of the times and contents of texts, emails, messages, as well as saved user names and passwords, cellular network provider/carrier information, user/owner account information, calendar events, contact lists, SMS (short message service) & MMS (Multimedia messaging service), call log details, e-mail accounts, internet web browsing activity, GPS (Global Positioning System) information, IP (Internet Protocol) Connections, user generated notes, digital photographs, video files, audio files, user generated dictionaries, wireless network connections, sync files, and voicemails.

26. Finally, there is probable cause to search for and seize the contacts lists from Verne's cell phone as it will help to establish with whom he was communicating, thereby making the attribution evidence intelligible. It will also show whether Employee 1 and Employee 1's wife were among Verne's contacts, itself a matter of evidentiary significance.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or

traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage

media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of

flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

28. Based on my training, experience, and research, I know that an iPhone, like the Verne iPhone, has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. Through my experience, I have located and recovered evidence of criminal violations in electronic devices, including cellular telephones, after a substantial period of time.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Verne iPhone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Verne iPhone because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* The Verne iPhone was seized on Friday, August 2, 2024, at the time of Verne's arrest in Fort Lauderdale, Florida, and it was processed and secured by FBI in Florida. In the days that followed, Verne's attorney in Philadelphia, Pennsylvania, inquired about the phone, asking if it would be available to Verne at his

arraignment on Thursday, August 8, 2024, in Philadelphia. On the day of the arrest, I requested that the Verne iPhone be sent from Florida to FBI Philadelphia. FBI Florida shipped the Verne iPhone through a private delivery service, and the phone arrived in Philadelphia, Pennsylvania, on August 7, 2024. As stated above, the Verne iPhone is now in a secure storage space at the FBI in Philadelphia, Pennsylvania. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Lorelei Schreier
Lorelei Schreier
Special Agent
Federal Bureau of Investigation

Sworn before me telephonically,

Carol Sandra Moore Wells
Date: 2024.08.07 13:57:41 -04'00'

HONORABLE CAROL S. WELLS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a black Apple iPhone, assigned telephone number ending in 0220 ("Verne iPhone"). The Verne iPhone is currently located in a secure storage space at the Federal Bureau of Investigation, 600 Arch Street, Philadelphia, Pennsylvania.

This warrant authorizes the forensic examination of the Verne iPhone for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and information on the Verne iPhone described in Attachment A that relate to violations of 18 U.S.C §§ 1513(e) (witness retaliation), 1512(b)(1) (witness intimidation), and 18 U.S.C. § 2, involving Josh S. Verne, on September 12, 2020, and the three weeks before and three weeks after September 12, 2020, including:

a. any information related to incoming and outgoing phone calls to the Verne iPhone;

b. any information related to incoming and outgoing text messages, including iMessages, on the Verne iPhone, other than privileged attorney-client communications;

c. contact lists and any other information to identify the source of the phone calls and text messages;

d. any information related to Verne's participation in the reverse proffer meeting on September 12, 2020, other than privileged attorney-client communications; and

e. any information related to Verne's contact or communications with potential witnesses in the federal criminal investigation of Verne, including Employee 1 and Employee 1's wife.

2. Evidence of user attribution showing who used or owned the Verne iPhone at the time the things described in this warrant were created, edited, or deleted, such as the times and contents of texts, emails, messages, as well as saved user names and

passwords, cellular network provider/carrier information, user/owner account information, calendar events, contact lists, SMS (short message service) & MMS (Multimedia messaging service), call log details, e-mail accounts, internet web browsing activity, GPS (Global Positioning System) information, IP (Internet Protocol) Connections, user generated notes, digital photographs, video files, audio files, user generated dictionaries, wireless network connections, sync files, and voicemails.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title